REMARKS

Claims 1 through 36 have been cancelled and replaced by new claims 37 through 43 to more distinctly claim and particularly point out the invention. No new matter has been added. Before discussing these claims in more detail, Applicants provide the following discussion to better contrast the claimed inventions from the prior art.

In conventional digital rights management (DRM) systems, the host (such as as PC) is where the DRM processing is conducted. This location is inherently vulnerable to hacking. Thus there is a need for improved DRM systems. However, content users have legitimate expectations as well that should not be violated by an overly-restrictive DRM system. To address this need in the art, Applicants have provided a DRM system in which DRM "intelligence" is incorporated into the storage engine. As opposed to conventional DRM systems that reside on the host, an integrated storage engine approach is far less vulnerable to hacking by a host system user – the user has no access to DRM functionality within the storage engine other than through reading and writing of secure content according to rules governed by the storage engine itself. The user knows that digital content may flow to and from the data storage medium but cannot access the "how" within the storage engine that enabled such movement. Moreover, the integration of the DRM system into the storage engine is advantageous in portable applications. Different host systems such as kiosks at a content provider retail outlet or a personal computer may be more readily modified to couple to the portable DRM-system-integrated storage engine.

Claim 37 reflects these advantageous properties of a DRM-integrated storage engine: For example, only after the authentication acts of "receiving at a storage engine a

certificate from the host device, the certificate containing a digital signature; authenticating the digital signature; receiving at the storage engine a file request from the authenticated host device, the file request being directed to a file stored on a storage medium accessible to the storage engine" can a host gain access to content on the storage medium. These acts are supported, for example, with respect to Figure 6 and the accompanying description on pages 29 and 30. As seen in Figure 6, the data storage engine generates a secure session key which is encrypted according to the host's public key. The host can only decrypt the secure session key if the host possesses the corresponding private key. As stated, for example, on page 45, upon authentication the storage engine "provides functionality to the CKDRM and TPDRM methods, including lock/unlock, CKDRM play, CKDRM copy permissions, and CKDRM copy permissions." Further description of how this functionality is implemented by the storage engine is set forth, for example, on pages 45 through 84. Claim 37 thus has support for the limitations of "within the storage engine, reading security metadata associated with the file from the storage medium, the security metadata containing at least one rule governing access to the file; within the storage engine, applying the at least one rule to the file request from the host device; and if the application of the at least one rule provides a failing result, denying the file request." For example, should the at least one rule govern indicate a file is locked as set forth, for example, on pages 51 through 52 of the application, the storage engine will deny access to the host unless the host has proper authorization to submit an unlock command.

In sharp contrast to the advantageous storage-engine-centric DRM method of claim 37, the cited prior art merely discloses conventional host-based DRM systems. For

example, consider the Ginter reference (USP 6,389,402). Ginter discloses that hosts comprise a "secure processing unit (SPU)" as set forth in Col. 59. This SPU comprises a typical PC architecture as seen in Figure 9. It is this SPU that "stores important information securely" as discussed in Col. 59, lines 43-44. Because this SPU (the host) is performing the DRM, Ginter goes to great pains to try and protect it from prying eyes: see Col. 63, lines 55-56: "SPU 500 may be surrounded by a tamper-resistant hardware security barrier." As discussed above, this is the great flaw of host-based DRM systems – there vulnerability to hacking. In sharp contrast, the storage engine controls access as recited in claim 37. Accordingly, claim 37 is patentable over the Ginter reference.

Because claims 38 through 41 depend upon claim 37 either directly or indirectly, they are patentable over Ginter for at least the same reasons. No new matter has been entered. For example, claim 38 limits the at least one rule to comprises a plurality of rules. Support for such a limitation is discussed above. Claim 39 limits the storage medium to be an optical disk as discussed for example on page 88, line 2. Claim 40 limits the application of the at least one rule act to comprise checking play privileges for the host device as described, for example, on page 49. Claim 42 limit claim 37 to further include the act of granting the file request if the application of the at least one rule was successful: for example, granting the play request pursuant to checking the play privileges of the host.

Claim 42 is directed to a storage device configured to apply the method discussed with respect to claim 37. Accordingly claim 42 is patentable over the Ginter reference as discussed above. Claim 43 limits the storage medium to be an optical disk as discussed above and is thus also patentable over the Ginter reference.

CONCLUSION

For the above reasons, pending Claims 37 through 43 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

Certification of Facsimile Transmission
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Linda Bolter — August 27, 2004
Linda Bolter — Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicants
Registration No. 42,622